

1 **WO**

2  
3  
4  
5  
6 **IN THE UNITED STATES DISTRICT COURT**  
7 **FOR THE DISTRICT OF ARIZONA**  
8

9 Federal Trade Commission,

10 Plaintiff,

11 v.

12 James D. Noland, Jr., et al.,

13 Defendants.  
14

No. CV-20-00047-PHX-DWL

**ORDER**

15 **INTRODUCTION**

16 In May 2019, Defendant James Noland (“Noland”) discovered, via the inadvertent  
17 disclosure of a bank subpoena, that the FTC was conducting an investigation of him and  
18 his business, Success By Health (“SBH”). When the FTC learned its investigation was no  
19 longer covert, it specifically advised Noland and SBH to preserve relevant documents.

20 They did no such thing. The day after learning about the FTC’s investigation,  
21 Noland instructed the other members of SBH’s leadership team, Defendants Lina Noland,  
22 Thomas Sacca (“Sacca”), and Scott Harris (“Harris”) (together with Noland, the  
23 “Individual Defendants”), to start using a pair of encrypted communications platforms  
24 called Signal and ProtonMail. After doing so, the Individual Defendants stopped using  
25 their previous messaging platforms for work-related communications, apparently turned  
26 on Signal’s “auto-delete” function, and then proceeded to exchange an untold number of  
27 messages related to SBH’s business.

28 In January 2020, after completing its investigation, the FTC filed this action. At the

1 same time, the FTC sought and obtained a temporary restraining order (“TRO”) that,  
2 among other things, appointed a receiver to assume control over SBH, required the  
3 Individual Defendants to produce their electronic communications, and required the  
4 Individual Defendants to turn over the mobile devices they had used to operate the  
5 business. Notwithstanding these orders, the Individual Defendants did not initially turn  
6 over their mobile devices and did not produce any Signal communications. Additionally,  
7 during a post-TRO deposition, Noland failed to disclose the Signal and ProtonMail  
8 accounts in response to direct questioning about the existence of any encrypted  
9 communications platforms.

10 It gets worse. It has now come to light that, during the months following the  
11 issuance of the TRO, Noland used his ProtonMail account to provide third-party witnesses  
12 with what can be construed as a script to follow when drafting declarations the Individual  
13 Defendants wished to submit in support of their defense. These communications only came  
14 to light by fortuity, when one of the recipients anonymously disclosed them to the FTC.

15 Finally, in August 2020, just as they were about to belatedly turn over their mobile  
16 devices for imaging, the Individual Defendants deleted the Signal app from their phones in  
17 coordinated fashion. As a result, neither side’s forensic specialists have been able to  
18 recover any of the Signal communications the Individual Defendants sent and received  
19 between May 2019 and August 2020.

20 Based on all of this, the FTC now moves for the imposition of spoliation sanctions.  
21 (Doc. 259.) The motion is fully briefed (Docs. 276, 277) and neither side requested oral  
22 argument. For the following reasons, the motion is granted. The Individual Defendants’  
23 systematic efforts to conceal and destroy evidence are deeply troubling and have cast a pall  
24 over this action.

### 25 **RELEVANT FACTUAL AND PROCEDURAL BACKGROUND**

26 This case concerns the business activities of SBH, “an affiliate-marketing program  
27 that sells coffee products and other nutraceuticals through its online platform and network  
28 of affiliates.” (Doc. 106 at 1-2.) SBH is an unincorporated division of Success by Media

1 Holdings Inc (“SBM”). (*Id.* at 1-2, 6.) The FTC alleges, among other things, that SBH  
 2 operated as an illegal pyramid scheme and that the Individual Defendants, who held various  
 3 leadership roles within SBH, made false statements to SBH’s affiliates. (Doc. 3.)

4 On April 26, 2019, the FTC issued a subpoena to Wells Fargo seeking financial  
 5 information related to Noland and SBH. (Doc. 259-1 at 26-42.)

6 On or around May 15, 2019, Wells Fargo inadvertently disclosed the subpoena to  
 7 Noland. (Doc. 8-19 at 5 ¶¶ 13-15; Doc. 259-1 at 25.)

8 On May 16, 2019, one day after inadvertently learning about the FTC’s subpoena,  
 9 Noland sent an invitation to Harris to install “Signal,” a mobile messaging application that  
 10 emphasizes user privacy,<sup>1</sup> and separately sent a message to the “SBH Leadership Council”  
 11 (which included Noland, Harris, and Sacca) stating that he had “[j]ust sent y’all an  
 12 important invite to an app you need to install.” (Doc. 259-1 at 4-5 ¶¶ 7-8, 14 ¶ 19.) The  
 13 evidence proffered by the FTC, which the Individual Defendants do not dispute, suggests  
 14 that Noland, Harris, and the other Individual Defendants began using Signal for the first  
 15 time that same day. (Doc. 228-1 at 2-3; Doc. 259-1 at 136, 147; Doc. 276-1 at 46, lines 3-  
 16 12.) Thereafter, Noland and the other Individual Defendants began encouraging SBH  
 17 employees and affiliates to install the Signal app. (Doc. 259-1 at 7-17 ¶¶ 15-23.) It appears  
 18 the Individual Defendants also turned on Signal’s “auto-delete” function after installing the  
 19 app, such that messages exchanged via Signal were not preserved.<sup>2</sup>

20 Around the same time he started using Signal, Noland also began using  
 21 “ProtonMail,” a Switzerland-based encrypted email service. (Doc. 259-1 at 22 ¶ 38, 140.)

22 <sup>1</sup> Signal, as noted, emphasizes user privacy. (Doc. 259-1 at 20 ¶ 32, 111-12.) The  
 23 key security features of Signal are its end-to-end encryption and its assurance that all  
 24 messaging data, including the content of the communications, cannot be tracked or  
 observed by Signal itself or any party that does not have access to the user’s device. (*Id.*  
 at 111-12, 119-20.)

25 <sup>2</sup> In an October 2020 letter to the FTC, the Individual Defendants’ counsel made  
 26 statements about the use of the auto-delete function. (Doc. 228-2 at 42 [“Our clients inform  
 27 us that they set all conversations to auto-delete with the exception of conversations with  
 28 their attorney.”].) During a subsequent deposition, Noland was asked further questions on  
 this topic. (Doc. 259-1 at 139-40.) In response, Noland seemed to confirm the accuracy  
 of his counsel’s statement in the letter. (*Id.*) Unfortunately, the Individual Defendants’  
 deletion of the Signal app from their phones has made it impossible to forensically verify  
 whether and when the auto-delete feature was, in fact, enabled. (Doc. 228-2 at 42.)

1 ProtonMail, like Signal, emphasizes user privacy. (*Id.* at 20 ¶ 33, 115-17.) Thereafter,  
 2 Noland and the other Individual Defendants encouraged SBH employees and affiliates to  
 3 use ProtonMail. (Doc. 228-2 at 5 ¶ 14, 6 ¶ 15; Doc. 259-1 at 12 ¶ 17, 13 ¶ 18, 15 ¶ 20, 22  
 4 ¶ 38.)

5 On May 20, 2019, Noland, through his attorney, contacted the FTC and offered to  
 6 cooperate with the FTC’s investigation. (Doc. 8-19 at 5 ¶ 15; Doc. 259-1 at 44, 138-39.)

7 On May 29, 2019, the FTC responded by stating that it did “not have any requests”  
 8 at that time and that “[Noland] and the company should suspend any ordinary course  
 9 destruction of documents, communications, and records.” (Doc. 259-1 at 44.)

10 Throughout the remainder of 2019, the Individual Defendants instructed each other  
 11 (as well as SBH employees and affiliates) to use Signal or ProtonMail for “anything  
 12 sensitive” or “important things.” (Doc. 259-1 at 12 ¶ 17, 18 ¶ 24.) Additionally, some of  
 13 the Individual Defendants’ unencrypted text messages simply referenced “Signal” or  
 14 “ProtonMail” or directed persons to check Signal or ProtonMail messages. (Doc. 259-1 at  
 15 13, ¶ 17, 16 ¶¶ 20-21, 18 ¶ 24.)

16 On January 8, 2020, the FTC initiated this action. (Doc. 3.) That same day, the  
 17 FTC moved for an *ex parte* TRO, which the Court substantially granted (Docs. 19, 38).<sup>3</sup>  
 18 The TRO was served on the Individual Defendants shortly thereafter. (Docs. 44-49.) In  
 19 the TRO, the Court appointed Kimberly Friday to serve as the receiver (the “Receiver”) of  
 20 SBH and affiliated entities. (Doc. 38 at 16.)<sup>4</sup> The TRO required the Individual Defendants  
 21 to, among other things, “immediately transfer or deliver to the [Receiver] possession,  
 22 custody, and control of . . . [a]ll Documents of or pertaining to the Receivership Entities,  
 23 including all communications occurring via electronic mail, electronic messaging service,  
 24 or encrypted messaging service . . . .” (Doc. 21 at 21; Doc. 38 at 21.) The TRO also  
 25 required the Individual Defendants to turn over “[a]ll keys, codes, user names and  
 26 passwords necessary to gain or to secure access to any Assets or Documents of or

27 <sup>3</sup> The TRO was later amended. (Docs. 20, 21.) The final, unsealed version of the  
 28 TRO was filed on January 17, 2020. (Doc. 38.)

<sup>4</sup> Friday has since been replaced as the Receiver by Peter S. Davis. (Doc. 395).

1 pertaining to the Receivership Entities, including access to their business premises, means  
 2 of communication, . . . encrypted messaging services . . . , or other property.” (Doc. 21 at  
 3 21-22; Doc. 38 at 22.) The same obligations applied under the preliminary injunction  
 4 entered on February 28, 2020. (Doc. 109 at 17-18.)

5 On February 5, 2020, Noland participated in a post-TRO deposition. (Doc. 259-1  
 6 at 130.) During the deposition, Noland was specifically asked about his use of encrypted  
 7 communication platforms. (*Id.*) In response, he failed to disclose the existence of his  
 8 Signal and ProtonMail accounts:

9 Q: Have you ever used any type of encrypted communications to  
 10 conduct Success by Media business?

11 A: I’m not sure what you mean, sir.

12 Q: Have you used any type of phone application or software system that  
 13 encrypts the substance of the communication from point to point?

14 A: I mean, I think it’s like standard practice now. I don’t know. It’s  
 15 standard practice.

16 Q: Do you know that in your course of your work for Success by  
 17 Media?

18 A: I don’t know. Whatever communication. I mean, it’s a phone call.  
 19 The encrypted, what Verizon offers.

20 Q: Do you do anything separately to encrypt your communications  
 21 apart from what a Verizon provider may do on their end?

22 A: *Just have, you know, I think WhatsApp uses that now.*

23 (*Id.*, emphasis added.)

24 On March 19, 2020, the Individual Defendants provided their initial discovery  
 25 responses pursuant to the Court’s Mandatory Initial Discovery Pilot Project (“MIDP”).  
 26 Among other things, the MIDP requires a party to “[l]ist the documents, *electronically*  
 27 *stored information* (‘ESI’), tangible things, land, or other property known by you to exist,  
 28 whether or not in your possession, custody or control, that you believe may be relevant to  
 any party’s claims or defenses.” D. Ariz. G.O. 17-08 § B.3 (emphasis added). In their  
 responses, however, the Individual Defendants did not disclose the existence of any Signal  
 or ProtonMail messages. (Doc. 259-1 at 95-96.)

On May 29, 2020, Noland used his ProtonMail account to send an email entitled “Declarations Needed from SBH Affiliates.” (Doc. 228-2 at 8.) Although the recipient’s name is blacked out in the copy of the email that has been provided to the Court, the FTC asserts (and the Individual Defendants do not deny) that the recipient was Robert Mehler, who previously served as SBH’s director of sales. (Doc. 259 at 13.) In the body of the email, Noland asked Mehler to solicit declarations from SBH affiliates and provided a list of information that affiliates should include in their declarations, such as “The purpose of the company is to sell product,” “Each affiliate and user of the product believes there is a healthful or positive effects [sic] that comes from using the SBH products,” “Affiliates have found financial freedom because of their ability to earn commissions from the sale of products,” and “Does not feels [sic] as though any SBH Affiliate received misrepresentations have been made to them by Success By Health.” (Doc. 228-2 at 8.)<sup>5</sup> After sending this email, Noland deleted it without disclosing it to the FTC. (Doc. 276 at 3 [Individual Defendants’ response, conceding that Noland deleted and failed to produce this email].) The email only happened to come to the FTC’s attention months later, via “an SBH Affiliate who requested to remain anonymous.” (Doc. 259 at 13 n.10.)

On August 18-19, 2020, the Individual Defendants provided their cell phones to be forensically imaged. (Doc. 228-1 at 2; Doc. 259-1 at 140.) The day beforehand, all four Individual Defendants deleted the Signal app from their phones. (Doc. 228-1 at 2-3; Doc. 259-1 at 140.) The Individual Defendants took this step without the knowledge or approval of their counsel, the Receiver, or the FTC. Indeed, during post-destruction correspondence with the FTC, the Individual Defendants’ counsel stated that “our clients, without our knowledge, uninstalled the Signal app a few days before their phones were imaged. . . . [We] had a very unpleasant conversation[] with our clients this morning about what happened.” (Doc. 228-2 at 21-22.) The deletion of Signal has resulted in a total inability of the parties or outside forensic experts to recover the contents of the Signal messages.

---

<sup>5</sup> The Court notes that, in the months after Noland sent this email from his ProtonMail account, the Individual Defendants filed an array of declarations from affiliates that seemed to closely track the statements in Noland’s email. (*See, e.g.*, Docs. 146-1, 146-2.)

(Doc. 228-2 at 17-19, 21-22.)

In late September or early October 2020, the FTC belatedly learned about the Individual Defendants' use of Signal. (Doc. 228 at 6; Doc. 259-1 at 3 ¶ 5.) The discovery occurred after the Individual Defendants produced a batch of discovery materials to the FTC. (*Id.*) In that production, the Individual Defendants included several Excel spreadsheets containing their text message communications. (Doc. 259-1 at 3 ¶ 5.) Among these were 7,507 WhatsApp messages exchanged within the SBH Leadership Council—a group text message thread consisting of Noland, Harris, Sacca, and nonparty Luke Curry (“Curry”).<sup>6</sup> (*Id.* at 4-5 ¶¶ 7-8.) Of these 7,507 messages, 7,505 were sent between September 2, 2017 and May 16, 2019, with the remaining two sent in August 2019. (*Id.*) All contact between Noland and the SBH Leadership Council (via the WhatsApp thread) ceased on May 16, 2019, while some messages between Sacca and Harris continued. (*Id.* at 4-7 ¶¶ 7-12.) According to the FTC’s investigator, Noland’s communications with the SBH Leadership Council group chat averaged 20.82 communications per day in 2017, 10.03 communications per day in 2018, and 13.80 communications per day in 2019 before all communications on that platform dwindled after May 16, 2019. (*Id.* at 6 ¶¶ 12-14.) Noland and other SBH leaders also exchanged thousands of text messages through similar iOS messaging groups from 2017 to May 16, 2019. (*Id.* at 5-6 ¶¶ 9-11.) As noted, May 16, 2019 is when Noland invited the other members of the SBH Leadership Council to install Signal, and from that point forward Noland, Harris, and Sacca encouraged each other and SBH employees and affiliates to use Signal and ProtonMail for “anything sensitive” and “important things.” (*Id.* at 7 ¶ 15, 10 ¶ 16, 12-14 ¶¶ 17-18, 16-18 ¶¶ 21-24.)

The FTC asserts that the WhatsApp and iOS messages from before May 16, 2019 reveal that the Individual Defendants and their associates discussed relevant matters—including the Individual Defendants’ focus on recruiting, substantial income claims, and

---

<sup>6</sup> In its moving papers, the FTC asserts that Curry was only part of the SBH Leadership Council group chat until October 2018 (Doc. 259 at 1) but does not attach evidence showing that Curry left the SBH Leadership Council at that time. The FTC’s declaration indicates that Curry remained part of the WhatsApp chat group through 2019. (Doc. 259-1 at 4-6 ¶¶ 7-11.)



1 actual financial results—on those platforms before the apparent switch to Signal and  
2 ProtonMail. (Doc. 259 at 2; Doc. 259-1 at 7-15 ¶¶ 15-20.)

3 On October 30, 2020, after the parties’ counsel became aware of the unavailability  
4 of the Individual Defendants’ Signal and ProtonMail messages, the Individual Defendants’  
5 counsel sent a letter to 22 SBH employees or affiliates seeking their Signal and/or  
6 ProtonMail communications with the Individual Defendants on relevant topics. (Doc. 259-  
7 1 at 18-19 ¶¶ 27-28, 47, 61.) Ten responded. (*Id.* at 18-19 ¶¶ 27-28, 49-59.) All said they  
8 did not have any Signal or ProtonMail messages to produce. (*Id.* at 49-59.) Several  
9 attributed the absence of messages to their use of Signal’s auto-delete feature (*id.* at 51-53,  
10 55) or their suspending or clearing of ProtonMail accounts (*id.* at 53, 55).<sup>7</sup>

11 In December 2020, the FTC deposed the Individual Defendants. (*Id.* at 136-43;  
12 Doc. 276-1 at 28-29, 38, 46; Doc. 277-1 at 6.) During these depositions, the FTC asked  
13 various questions regarding the use of Signal and ProtonMail. (*Id.*) Noland admitted that  
14 he installed Signal on his phone on or around May 16, 2019 and, around the same time,  
15 asked Harris and Sacca to install Signal on their phones. (Doc. 259-1 at 136.) Harris and  
16 Sacca recalled being asked to install Signal and installing it around this time. (Doc 276-1  
17 at 38, 46.) Sacca further testified that Noland informed him about receiving the FTC bank  
18 subpoena in May 2019. (*Id.* at 48-49.) Noland, Sacca, and Harris also acknowledged that  
19 they deleted Signal from the phones just before imaging. (*Id.* at 19-21, 50-51.) Sacca  
20 testified that the deletion was part of a coordinated plan between himself, Harris, and  
21 Noland. (*Id.* at 50-51.) Noland provided a similar account of the joint plan to delete the  
22 app. (*Id.* at 20 [discussing “a conversation with Scott and Tommy” that preceded the  
23 deletion].)

24 On January 28, 2021, the FTC filed the motion for sanctions. (Doc. 259.) The  
25 motion thereafter became fully briefed. (Docs. 276, 277.)

---

26 <sup>7</sup> One of the individuals who responded was Mehler. (Doc. 259-1 at 51.) In his  
27 response, Mehler stated: “I also have no communication via proton mail with the  
28 executives regarding SBH business as . . . there was no ‘company business’ to discuss.”  
(*Id.*) Mehler did not, in other words, disclose and produce the ProtonMail email that was  
apparently sent to him by Noland on May 29, 2020.



## DISCUSSION

The FTC seeks an adverse inference against the Individual Defendants pursuant to Rule 37(e)(2) of the Federal Rules of Civil Procedure based on their intentional spoliation of evidence. (Doc. 259 at 13-17.)

### I. Legal Standard

Rule 37(e) was “completely rewritten” in 2015 to “provide[] a nationally uniform standard for when courts can give an adverse inference instruction, or impose equally or more severe sanctions, to remedy the loss of ESI.” *See generally* 1 Gensler, Federal Rules of Civil Procedure, Rules and Commentary, Rule 37, at 1194 (2021). The text of Rule 37(e)(2) now provides:

If electronically stored information that should have been preserved in the anticipation or conduct of litigation is lost because a party failed to take reasonable steps to preserve it, and it cannot be restored or replaced through additional discovery, the court:

. . .

- (2) only upon finding that the party acted with the intent to deprive another party of the information’s use in the litigation may:
  - (A) presume that the lost information was unfavorable to the party;
  - (B) instruct the jury that it may or must presume the information was unfavorable to the party; or
  - (C) dismiss the action or enter a default judgment.

(*Id.*) A court cannot rely on its inherent authority (or state law) when deciding whether sanctions based on the loss of ESI are appropriate—the standards supplied by Rule 37(e) are exclusive. Gensler, *supra*, at 1198. *See also Newberry v. County of San Bernardino*, 750 Fed. App’x 534, 537 (9th Cir. 2018) (“The parties framed the sanctions issue as invoking the district court’s inherent authority. However, at the time the sanctions motion was filed, sanctions were governed by the current version of Rule 37(e) . . . [which] therefore foreclose[d] reliance on inherent authority to determine whether terminating sanctions were appropriate.”) (citations and internal quotation marks omitted).

1 A party seeking sanctions under Rule 37(e) has a threshold duty to show that the  
 2 ESI at issue was, in fact, lost or destroyed. Fed. R. Civ. P. 37(e) advisory committee’s note  
 3 to 2015 amendment (“The new rule applies only . . . when [ESI] is lost.”). If such a  
 4 showing has been made, the court must then determine whether “(1) the ESI should have  
 5 been preserved in the anticipation or conduct of litigation; (2) the ESI is lost because a  
 6 party failed to take reasonable steps to preserve it; and (3) the ESI cannot be restored or  
 7 replaced through additional discovery.” *Porter v. City & County of San Francisco*, 2018  
 8 WL 4215602, \*3 (N.D. Cal. 2018) (cleaned up). *See also* Fed. R. Civ. P. 37(e) advisory  
 9 committee’s note to 2015 amendment (“The new rule applies only if the lost information  
 10 should have been preserved in the anticipation or conduct of litigation and the party failed  
 11 to take reasonable steps to preserve it.”).

12 If each of these questions is answered in the affirmative, the next inquiry under Rule  
 13 37(e)(2) is whether the nonmovant “acted with the intent to deprive another party of the  
 14 information’s use in the litigation.” *Porter*, 2018 WL 4215602 at \*3. Unlike Rule 37(e)(1),  
 15 Rule 37(e)(2) “does not include a requirement that the court find prejudice to the party  
 16 deprived of the information. This is because the finding of intent required by the  
 17 subdivision can support not only an inference that the lost information was unfavorable to  
 18 the party that intentionally destroyed it, but also an inference that the opposing party was  
 19 prejudiced by the loss of information that would have favored its position. Subdivision  
 20 (e)(2) does not require any further finding of prejudice.” Fed. R. Civ. P. 37(e) advisory  
 21 committee’s note to 2015 amendment.

22 If such intent is found, the Court has discretion to impose any of the sanctions  
 23 authorized in subsections (e)(2)(A)-(C) (*i.e.*, an adverse inference, an adverse-inference  
 24 jury instruction, or a terminating sanction). However, “[f]inding an intent to deprive  
 25 another party of the lost information’s use in the litigation does not require a court to adopt  
 26 any of the measures listed in subdivision (e)(2). The remedy should fit the wrong, and the  
 27 severe measures authorized by this subdivision should not be used when the information  
 28 lost was relatively unimportant or lesser measures such as those specified in subdivision

(e)(1) would be sufficient to redress the loss.” *Id.*

“[T]he applicable standard of proof for spoliation in the Ninth Circuit appears to be by a preponderance of the evidence.” *Compass Bank v. Morris Cerullo World Evangelism*, 104 F. Supp. 3d. 1040, 1052-53 (S.D. Cal. 2015). *See also Singleton v. Kernan*, 2018 WL 5761688, \*2 (S.D. Cal. 2018) (“A party seeking sanctions for spoliation of evidence has the burden of establishing [spoliation of non-electronic records] by a preponderance of the evidence[.]”). The Court is the appropriate finder of fact on a Rule 37(e) motion. *Mannion v. Ameri-Can Freight Sys. Inc.*, 2020 WL 417492, \*4 (D. Ariz. 2020). *See also Adriana Int’l Corp. v. Thoenen*, 913 F.2d 1406, 1408 (9th Cir. 1990) (“The imposition of discovery sanctions pursuant to [Rule 37] is reviewed for abuse of discretion. Absent a definite and firm conviction that the district court made a clear error in judgment, this court will not overturn a Rule 37 sanction. Findings of fact related to a motion for discovery sanctions are reviewed under the clearly erroneous standard. If the district court fails to make factual findings, the decision on a motion for sanctions is reviewed de novo.”) (citations omitted).

## II. Analysis

### A. **Whether ESI Was Lost**

#### 1. Signal

It is undisputed that the Individual Defendants deleted the Signal app and Signal messages. (Doc. 230 at 2; Doc. 259-1 at 139-40, 143, 148; Doc. 276 at 1; Doc. 277-1 at 6.) It is also undisputed that the Individual Defendants used Signal to communicate about SBH business. (*See, e.g.*, Doc. 259-1 at 13 ¶ 18, 138-41; Doc. 276 at 1-2; Doc. 276-1 at 12-14.) For example, during his December 2020 deposition, Noland stated that he communicated or likely communicated with Harris, Sacca, and various “Staff members” on Signal. (Doc. 159-1 at 138.) Noland also acknowledged that he discussed SBH business on Signal “from time to time.” (*Id.*) He further admitted that he continued to use Signal after the TRO in this case was issued. (*Id.* at 139.)

The parties disagree about the precise mechanism by which the Signal messages were lost. The Individual Defendants assert that they used Signal’s “auto-delete” feature,

1 meaning messages would disappear from users’ devices shortly after they were read by the  
 2 recipient. (Doc. 276 at 1-2; Doc. 276-1 at 18-19.) The FTC sounds a note of skepticism  
 3 about the Individual Defendants’ use of auto-delete because the Individual Defendants  
 4 belatedly offered this explanation for the loss of the messages “[w]eeks after admitting to  
 5 deleting the Signal apps.” (Doc. 259 at 11 n.5.) The FTC also considers this explanation  
 6 “implausible” for a variety of reasons (Doc. 277 at 4-6) but argues that, regardless of  
 7 whether the auto-delete function was enabled, the bottom line is that the Individual  
 8 Defendants caused ESI to be lost. (*Id.* at 4, 8-9.)

9       The Court agrees with the FTC that, for the purposes of the threshold inquiry of  
 10 whether any ESI was lost, it is irrelevant whether the Signal messages were lost in one fell  
 11 swoop in August 2020 (when the Individual Defendants deleted the Signal app) or whether  
 12 the loss occurred on a continuous basis from May 2019 through August 2020 (due to the  
 13 Individual Defendants’ choice to turn on Signal’s auto-delete feature). Regardless of how  
 14 and when it occurred, Signal-related ESI was lost. *Cf. DR Distributors, LLC v. 21 Century*  
 15 *Smoking, Inc.*, 513 F. Supp. 3d 839, 931-33 (N.D. Ill. 2021) (“[A]utodelete functionality is  
 16 and has been a near ubiquitous feature in programs and email services that produce ESI,  
 17 leading to a phalanx of publications warning litigators of the need to clearly and adequately  
 18 inform their clients to investigate and turn off autodelete functions as part of their litigation  
 19 hold processes. It follows that in cases involving ESI, to satisfy their preservation duties,  
 20 parties must investigate and disable autodelete functions on email accounts (client and  
 21 web-based) at the onset of litigation if those accounts reasonably contain relevant  
 22 information and it is reasonable under the circumstances of the case to do so. . . . [P]arties  
 23 that ignore their obligations to reasonably investigate the possibility of or disregard  
 24 autodelete functions run the risk of destroying relevant evidence and visiting prejudice  
 25 upon their litigation adversaries, thereby earning sanctions.”); The Sedona Conference, *The*  
 26 *Sedona Conference Primer on Social Media, Second Edition*, 20 Sedona Conf. J. 1, 90-91  
 27 (2019) (“A client’s use of ephemeral messaging for relevant communications after a duty  
 28 to preserve has arisen may be particularly problematic, as it would have the potential to

1 deprive adversaries and the court of relevant evidence.”)

2                   2.     ProtonMail

3             The FTC asserts that it uncovered a May 2020 email from Noland’s ProtonMail  
4 account providing instructions for declarations to be submitted to the Court in this action.  
5 (Doc. 228-2 at 3 ¶ 5, 8; Doc. 259 at 10 & n.3.) During meet-and-confer correspondence in  
6 October 2020, in response to questions about why the Individual Defendants had not  
7 produced this email, the Individual Defendants’ counsel admitted that Noland deleted it.  
8 (Doc. 228-2 at 29.) And in their response to the FTC’s motion for sanctions, the Individual  
9 Defendants again admit that Noland deleted it. (Doc. 276 at 3 n.3 [“Noland . . . deleted at  
10 least one post-TRO email from his new [ProtonMail] account . . . .”].)

11             Given this backdrop, it is clear that ProtonMail ESI was lost. Although the parties  
12 disagree about whether the loss extended beyond the May 2020 email, it is undisputed that  
13 at least one email was lost (although another version was found through other channels).<sup>8</sup>

14                   B.     **Duty To Preserve**

15             Sanctions are available under Rule 37(e) only if the loss of ESI occurred at a time  
16 when litigation was pending or reasonably foreseeable. Fed. R. Civ. P. Rule 37(e),  
17 advisory committee’s note to 2015 amendment (“The new rule applies only if the lost  
18 information should have been preserved in the anticipation or conduct of litigation . . . .  
19 Many court decisions hold that potential litigants have a duty to preserve relevant  
20 information when litigation is reasonably foreseeable. Rule 37(e) is based on this common-  
21 law duty; it does not attempt to create a new duty to preserve. The rule does not apply  
22 when information is lost before a duty to preserve arises.”). Further, the ESI must have  
23 been foreseeably relevant to the pending or foreseeable litigation. *Id.* (“Courts should  
24 consider the extent to which a party was on notice that litigation was likely *and that the*  
25 *information would be relevant.*”) (emphasis added).

26             ...

27  
28 <sup>8</sup> The Court clarifies that, even if the FTC hadn’t proved the loss of any ProtonMail  
ESI, it would impose an adverse-inference sanction based on the loss of Signal ESI.

1                   1.     Reasonable Foreseeability Of Litigation

2                   As the Ninth Circuit has explained, parties “engage in spoliation of documents as a  
3 matter of law only if they had ‘some notice that the documents were potentially relevant’  
4 to the litigation before they were destroyed.” *United States v. Kitsap Physicians Serv.*, 314  
5 F.3d 995, 1001 (9th Cir. 2002) (citation omitted). “This is an objective standard, asking  
6 not whether the party in fact reasonably foresaw litigation, but whether a reasonable party  
7 in the same factual circumstances would have reasonably foreseen litigation.” *Waymo LLC*  
8 *v. Uber Techs., Inc.*, 2018 WL 646701, \*14 (N.D. Cal. 2018) (internal quotation marks  
9 omitted). The reasonable foreseeability of litigation “is a flexible fact-specific standard  
10 that allows a district court to exercise the discretion necessary to confront the myriad  
11 factual situations inherent in the spoliation. This standard does not trigger the duty to  
12 preserve documents from the mere existence of a potential claim or the distant possibility  
13 of litigation. However, it is not so inflexible as to require that litigation be ‘imminent, or  
14 probable without significant contingencies.’” *Id.* at \*15 (quoting *Micron Tech., Inc. v.*  
15 *Rambus Inc.*, 645 F.3d 1311, 1320 (Fed. Cir. 2011)).

16                  The FTC argues the Individual Defendants’ preservation obligations arose in May  
17 2019, when they became aware of the FTC’s investigation. (Doc. 259 at 14 n.7.)  
18 Alternatively, the FTC argues the obligation arose no later than mid-January 2020, when  
19 they were served with the TRO. (*Id.* 14.) In response, the Individual Defendants argue  
20 that, although they learned about the FTC’s investigation in May 2019, they believed this  
21 investigation had concluded (due to the FTC’s rejection of Noland’s offer to cooperate).  
22 (Doc. 276 at 2-3.) The Individual Defendants do not address the propriety of continuing  
23 to erase Signal messages (and at least one ProtonMail email) after the TRO and preliminary  
24 injunction were entered. (*Id.*) The FTC replies that the Individual Defendants have  
25 admitted, at a minimum, that they violated their post-TRO preservation obligations, which  
26 encompass the duty to preserve any pre-TRO communications that were still available.  
27 (Doc. 277 at 4; *see also* Doc. 259 at 13-14 [“From the date of the TRO, Defendants had an  
28 obligation to preserve their SBM-related Signal and ProtonMail communications, both pre-

1 and post-TRO.”].)

2 The Court concludes that the Individual Defendants’ document preservation  
 3 obligations arose on May 29, 2019, when the FTC responded to Noland’s counsel’s email  
 4 by stating that Noland “and the company should suspend any ordinary course destruction  
 5 of documents, communications, and records.” (Doc. 259-1 at 44.) Although Noland  
 6 contends he subjectively believed the FTC’s rejection of his offer to cooperate signaled  
 7 that the investigation against him (and SBH) was closed, that was not an objectively  
 8 reasonable conclusion under the circumstances. Noland was aware that the FTC had  
 9 recently subpoenaed his bank records and was aware that the FTC had unambiguously  
 10 requested the suspension of document destruction. Additionally, Noland was aware that  
 11 he remained subject to the consent order arising from a previous FTC enforcement action,  
 12 *FTC v. Netforce Seminars*. (See generally Doc. 177 at 15 n.7.) It would be objectively  
 13 unreasonable, under these circumstances, to conclude that litigation is not probable and  
 14 that the retention of evidence is not required. *Cf. Blazer v. Gall*, 2019 WL 3494785, \*3  
 15 (D.S.D. 2019) (“The clearest signal of impending litigation came when Blazer’s [attorney]  
 16 . . . emailed an explicit request to Sheriff Boll for the production or preservation of any  
 17 recordings of Blazer . . . . While defendants posit that [the] email was not worded harshly  
 18 enough to trigger a duty to preserve, the email’s courteous phrasing does not nullify its  
 19 effectiveness as an indicator of impending litigation.”); *O’Berry v. Turner*, 2016 WL  
 20 1700403, \*3 (M.D. Ga. 2016) (“Here, the duty to preserve the driver’s log and additional  
 21 PeopleNet data arose at the very latest when Mr. Helms faxed a spoliation letter to  
 22 ADM[.]”); *Sampson v. City of Cambridge*, 251 F.R.D. 172, 181 (D. Md. 2008) (“It is clear  
 23 that defendant had a duty to preserve relevant evidence that arose no later than June 26,  
 24 2006, when plaintiff’s counsel sent the letter to defendant requesting the preservation of  
 25 relevant evidence, including electronic documents. At that time, although litigation had  
 26 not yet begun, defendant reasonably should have known that the evidence described in the  
 27 letter may be relevant to anticipated litigation.”) (internal quotation marks omitted).<sup>9</sup>

28 <sup>9</sup> Indeed, a duty to preserve may arise even where no preservation request has issued.  
*Clear-View Techs., Inc. v. Rasnick*, 2015 WL 2251005, \*1 (N.D. Cal. 2015) (“At times, a



At any rate, the availability of sanctions under Rule 37(e)(2) does not turn on whether the Individual Defendants’ preservation obligations arose in May 2019 or January 2020. It is undisputed that the Individual Defendants’ destruction of evidence continued after January 2020—after this date, Signal messages continued to be sent (and deleted), the May 2020 ProtonMail email from Noland to Mehler was sent and deleted, and the Individual Defendants worked together to delete the Signal app in coordinated fashion.

## 2. Reasonable Foreseeability Of The Relevance Of The Signal And ProtonMail Messages

The FTC acknowledges that the relevance of the lost ESI cannot be definitively ascertained (because it no longer exists) but argues that, in such circumstances, the Individual Defendants cannot assert any presumption of irrelevance. (Doc. 259 at 16-17.) The Individual Defendants respond that much, if not all, of the missing ESI is irrelevant. (Doc. 276 at 2-4.) First, they argue that the information lost when they deleted Signal was limited to the identities and contact lists of the persons with whom they communicated via the app and that such information “is not relevant and certainly not irretrievable.” (*Id.* at 2.) They also dispute the relevance of their post-TRO communications (but not, it appears, their pre-TRO communications) on the ground that “the overwhelming majority of evidence” in this case is public. (*Id.* at 3-4.) The FTC replies that the Individual Defendants do not dispute that the deleted messages included discussion of relevant matters such as SBH’s recruiting focus and income claims and that the Individual Defendants “do not get to pick the evidence that they think is sufficient for the FTC and then destroy the rest.” (Doc. 277 at 11.)

The FTC has the better side of these arguments. Noland admitted that he discussed SBH business matters on Signal “from time to time.” (Doc. 259-1 at 138.) Similarly, Sacca admitted that he used Signal to discuss SBH business. (Doc. 276-1 at 45.) This testimony, standing alone, strongly suggests that the deleted ESI was at least “potentially

---

defendant’s duty to preserve arises when plaintiff’s counsel provides a defendant with notice to preserve relevant evidence. However, a future litigant need not make such a request . . . .”) (footnote omitted).

relevant to the litigation.” *Leon v. IDX Sys. Corp.*, 464 F.3d 951, 959 (9th Cir. 2006). At any rate, “because the relevance of destroyed documents cannot be clearly ascertained because the documents no longer exist, a party can hardly assert any presumption of irrelevance as to the destroyed documents.” *Id.* (cleaned up). *See also Rasnick*, 2015 WL 2251005 at \*8 (“[T]he law presumes that spoliated evidence goes to the merits of the case . . . .”) (internal quotation marks omitted).

The lone deleted ProtonMail email that has been recovered further bolsters this conclusion. In that email, Noland asked Mehler to persuade SBH affiliates—that is, potential witnesses in this case—to make exculpatory representations about the purpose of the company, how Affiliates earn income from SBH, the absence of misrepresentations, and the like. (Doc. 228-2 at 8.) These topics are relevant to this litigation.<sup>10</sup> This raises an inference that other lost ESI addressed relevant topics, too. *Cf. Youngevity Int’l v. Smith*, 2020 WL 7048687, \*3 (S.D. Cal. 2020) (inferring spoliated text messages were relevant where the messages “were exchanged during periods significant to this litigation” and the text messages that had been produced were relevant).

The foreseeable relevance of the Signal and ProtonMail messages is also established by circumstantial evidence. For example, the FTC has submitted evidence establishing that the Individual Defendants’ pre-May 2019 communications via WhatsApp and iOS (on the SBH Leadership Council group chat and more generally) covered a variety of relevant topics. Then, in May 2019, almost immediately after learning they were under investigation by the FTC, the Individual Defendants started using Signal and ProtonMail and encouraged others to do so as well. Starting at the exact same time, the Individual

---

<sup>10</sup> Courts have sharply criticized the practice of secretly providing a script for third-party witnesses to follow during depositions or when drafting declarations. *Innospan Corp. v. Intuit Inc.*, 2011 WL 2669465, \*2-3 (N.D. Cal. 2011); *Hogan v. Higgins*, 2008 WL 3200252, \*3 (E.D.N.Y. 2008) (where plaintiff’s counsel wrote a detailed letter to a non-party witness that set forth the plaintiff’s theory of the case and asked the witness to offer testimony consistent with it, observing that “[t]he letter is, conservatively construed, a blatant attempt to coach a witness, and may reasonably be understood as an attempt to persuade a witness to change his testimony”). Although the Court reaches no conclusions about whether Noland’s May 2020 email to affiliates (via Mehler) constituted such a script, the optics are concerning.

1 Defendants' WhatsApp and iOS communications, on relevant topics or otherwise,  
 2 dwindled to almost nothing. The reasonable inference to be drawn from these undisputed  
 3 facts is that the Individual Defendants continued their discussions of relevant matters on  
 4 Signal and ProtonMail after switching over to those apps. The alternative inference—that  
 5 the Individual Defendants simply stopped communicating about anything related to their  
 6 business on any text-messaging platform, at the same time that they installed an encrypted  
 7 messaging service for the purpose of discussing “anything sensitive” and “important  
 8 matters”—strains credulity.

9 The FTC has thus carried its burden of showing the reasonably foreseeable  
 10 relevance of the destroyed ESI to this litigation.

### 11 C. Reasonable Steps To Preserve

12 The parties do not dispute that the Individual Defendants failed to take reasonable  
 13 steps to preserve the deleted communications. The Individual Defendants admit that they  
 14 “uninstalled the Signal messaging application just prior to having their phones forensically  
 15 imaged” (Doc. 276 at 1); that “Noland did not preserve some emails from an account that  
 16 was created after the temporary restraining order” (*id.*); and that “the un-installation of  
 17 Signal was intentional” (*id.* at 4). (*See also* Doc. 259-2 at 2 [Receiver’s Declaration].).

18 These admissions, coupled with the evidence outlined above, establish that the  
 19 Individual Defendants failed to take reasonable steps to preserve the Signal and ProtonMail  
 20 messages. This is true irrespective of whether the messages were lost because of  
 21 intentional deletion, through the intentional use of an auto-delete function, or some  
 22 combination thereof. *Cf. Paisley Park Enters., Inc. v. Boxill*, 330 F.R.D. 226, 233-34 (D.  
 23 Minn. 2019) (“There is no doubt that Staley and Wilson are the types of persons likely to  
 24 have relevant information, given their status as principals of RMA and owners of  
 25 Deliverance. Nor can there be any reasonable dispute as to the fact that their text messages  
 26 were likely to contain information relevant to this litigation. . . . Thus, the RMA  
 27 Defendants were required to take reasonable steps to preserve Staley and Wilson’s text  
 28 messages. The RMA Defendants did not do so. [They] did not suspend the auto-erase

1 function on their phones . . . [and it] takes, at most, only a few minutes to disengage the  
 2 auto-delete function on a cell phone. . . . Failure to follow [such] simple steps . . . alone is  
 3 sufficient to show that Defendants acted unreasonably.”); *Youngevity*, 2020 WL 7048687  
 4 at \*2 (“Defendants’ failure to prevent destruction by backing up their phones’ contents or  
 5 disabling automatic deletion functions was not reasonable because they had control over  
 6 their text messages and should have taken affirmative steps to prevent their destruction  
 7 when they became aware of their potential relevance.”).

#### 8 **D. Replaceability**

9 The next question under Rule 37(e) is whether the lost discovery “can[] be restored  
 10 or replaced through additional discovery.”

11 The FTC argues that the lost ESI is irreplaceable, because the deletion of the  
 12 messages and Signal app “leaves no way to recover them,” and further argues that although  
 13 the FTC and Individual Defendants’ counsel worked together to attempt to retrieve the  
 14 missing materials, those efforts were unsuccessful. (Doc. 259 at 17-18.) The Individual  
 15 Defendants do not dispute these points, acknowledging that the “forensic expert attempted  
 16 to recover the Signal data and could not.” (Doc. 276 at 2.) Of note, the Individual  
 17 Defendants’ counsel contacted 22 persons affiliated with SBH and asked them if they had  
 18 any ProtonMail or Signal communications with the Individual Defendants. (Doc. 259-1 at  
 19 46-61.) The 10 responding parties reported that they did not have any ProtonMail or Signal  
 20 communications with the Individual Defendants on their devices. (*Id.* at 49-59.)<sup>11</sup>

21  
 22 <sup>11</sup> The Individual Defendants argue that these persons’ failure to identify any  
 23 responsive Signal or ProtonMail communications “supports the individual defendants’  
 24 position that they were using the auto-delete feature, and did not intentionally (or in  
 25 actuality) destroy relevant evidence they were under a duty to preserve.” (Doc. 276 at 2.)  
 26 This argument is unpersuasive. The responding persons did not uniformly assert that they  
 27 had been using the auto-delete feature, instead often stating, without elaboration, that they  
 28 simply did not have any records of communications with the Individual Defendants in their  
 Signal or ProtonMail platforms. (*See, e.g.*, Doc. 259-1 at 49.) Further, only 10 out of 22  
 persons responded—the parties and the Court thus remain unaware of whether relevant  
 communications might be found on the remaining 12 persons’ devices. Finally, many of  
 the relevant communications likely would have been exchanged between the Individual  
 Defendants. That the 10 persons who responded had no relevant messages says nothing  
 about whether there may have been relevant communications between the Individual  
 Defendants.

1           The Court finds that the lost messages cannot be restored or replaced through  
2 additional discovery.

3           **E.       Finding Of Prejudice Unnecessary**

4           The FTC seeks sanctions under Rule 37(e)(2). (Doc. 259 at 13-17.) That provision,  
5 unlike Rule 37(e)(1), does not require a finding of prejudice to another party from loss of  
6 the information: “Rule 37(e)(2) does not require that the court find prejudice to the party  
7 deprived of the information. While the common law spoliation tests often required a  
8 showing of prejudice for the types of severe sanctions covered by Rule 37(e)(2), the  
9 Advisory Committee determined that there was no need to require a specific showing of  
10 prejudice once a finding of intent to deprive had been made.” 1 Gensler, *supra*, Rule 37,  
11 at 1203.

12           Thus, the Individual Defendants’ argument that the FTC has not shown it was  
13 prejudiced by the loss of information (Doc. 276 at 3-4) is unavailing. Rule 37(e)(2) does  
14 not require a finding of prejudice “because the finding of intent required by the subdivision  
15 can support not only an inference that the lost information was unfavorable to the party  
16 that intentionally destroyed it, but also an inference that the opposing party was prejudiced  
17 by the loss of information that would have favored its position.” Fed. R. Civ. P. 37(e),  
18 advisory committee’s note to 2015 amendment. The Court addresses potential prejudice,  
19 however, when discussing the appropriate sanction.

20           **F.       Intent To Deprive**

21           i.       The Parties’ Arguments

22           The parties dispute whether the Individual Defendants’ use of Signal and  
23 ProtonMail, and subsequent concealment and deletion of Signal and ProtonMail  
24 communications, constitute sufficient evidence of intent to deprive the FTC of these  
25 communications. (Doc. 259 at 15-16; Doc. 276 at 4.) The Individual Defendants assert  
26 that they switched from WhatsApp and iOS to Signal in May 2019 for an innocent reason—  
27 to avoid the hacking, eavesdropping, and infiltration efforts of former SBH associate Luke  
28

Curry<sup>12</sup> and “a small group of saboteurs.” (Doc. 276 at 3.)<sup>13</sup> The FTC argues this explanation is implausible. (Doc. 259 at 8 n.2.) The FTC’s investigator ran searches in the Individual Defendants’ document productions and found no communications suggesting that the Individual Defendants were concerned about hacking or other interference from Luke Curry in or around May 2019. (Doc. 259-1 at 21-22 ¶¶ 35-37.) Further, when later asked about the motivation to install Signal, Harris did not mention Luke Curry or any other specific hacking concerns—instead, he more generally stated that the Individual Defendants “wanted to make sure we had whatever was the most secure at the time to be able to – sometimes we send things like a copy of a driver’s license or someone asks for a Social Security number or we send pictures of our kids and things like that.” (*Id.* at 147-48.) Harris did, however, recall that at an unspecified time Noland raised concerns that the company and Noland’s personal phone were being hacked and mentioned that Luke Curry or his associates were responsible. (*Id.* at 148.) Sacca testified that he began to have concerns that his phone was hacked as early as 2016 or 2017 and that he was the person who strongly urged additional cyber and in-person security measures in light of the Luke Curry imbroglio. (Doc. 276-1 at 46-47.) Lina Noland also testified that hacking concerns tied to SBH’s problems with Luke Curry motivated the installation of Signal.

---

<sup>12</sup> The Individual Defendants obtained, by default, a preliminary injunction against Curry in Nevada state court in December 2018. (Doc. 276-1 at 53-55.) The preliminary injunction prevents Curry from advertising, promoting, or selling SBH competitor products; advertising, promoting, or selling SBH products; and making or disseminating disparaging remarks about any aspect of SBH, including SBH personnel. (*Id.* at 54.)

<sup>13</sup> During his December 2020 deposition, Noland provided the following explanation for why he chose to install the Signal app in May 2019: “Best I can remember, we were being – we were being – we were being attacked by different people that Luke Curry was stirring up, and it seemed to be some hacking going on. So we wanted to be able to try to help, you know, secure some of our messaging with the different attacks that were going on.” (Doc. 259-1 at 136.) Noland continued: “Like I said, that’s when we started noticing some issues that were going on with our phones. It seemed like – it just started ramping up more and more. We thought it was going to die down once we sued Luke in the Nevada court. We thought that that would – and he had a temporary restraining order on him, and then he had a preliminary injunction on him from the Nevada state court. . . . So we thought, with those measures from a judge – from a state judge, that maybe that would quiet some of that noise down, and it seemed to for a little bit period of time, and then it started to ramp back up. And then it looked like, as we got into the spring, the attacks started to ramp up.” (*Id.* at 137.) Noland testified that the same reasons motivated him to start using ProtonMail. (*Id.* at 140-41.)



1 (Doc. 276-1 at 29-30, 32.)

2 As for Noland's failure to disclose his ongoing use of Signal and ProtonMail during  
3 his February 2020 deposition, Noland contends that he was attempting to provide this  
4 information when he was cut off by the FTC's counsel. (Doc. 259-1 at 141-42.) The FTC  
5 asserts that this explanation is implausible. (Doc. 259 at 12.)

6 As for the Individual Defendants' deletion of the Signal app in August 2020, they  
7 contend it was justified because they didn't want the FTC to learn the names of the  
8 individuals who have been donating to their legal defense in this case. (Doc. 276 at 1-2;  
9 Doc. 259-1 at 140, 148; Doc. 276-1 at 50-51.) The FTC argues this explanation is  
10 implausible because "Defendants do not explain how a mere list of contacts and a phone  
11 log would somehow have revealed to the FTC who donated money to them." (Doc. 277 at  
12 7.) Further, the FTC argues, at other points in this litigation the Individual Defendants  
13 have represented that they don't know the identity of their donors, so it is inconsistent for  
14 them to aver that they don't know their donors' identities while simultaneously positing  
15 that they needed to delete Signal to protect those unknown persons' identities. (*Id.* at 7-8.)

16 ii. Analysis

17 The FTC has easily carried its burden of showing that the Individual Defendants  
18 acted with the intent to deprive the FTC of the information contained in the Signal and  
19 ProtonMail messages. The most decisive factor is the timing of the installation and use of  
20 Signal and ProtonMail. The Individual Defendants installed these apps in late May 2019,  
21 *one day* after Noland discovered the FTC was investigating him and SBH. The Individual  
22 Defendants would have the Court believe this timing was a coincidence—they happened  
23 to install elaborate encrypted privacy-focused apps immediately after discovering they  
24 were the subject of an FTC investigation because, around that same time, they noticed  
25 hacking attempts from Curry and his fellow "saboteurs." This explanation is incredible.  
26 Apart from the Individual Defendants' testimony, there is no documentary or other  
27 evidence supporting the notion that the Individual Defendants were being hacked at this  
28 time. (Doc. 259-1 at 21-22 ¶¶ 35-37.)



1           The plausibility of this explanation is further undermined by Noland’s failure to  
 2       disclose the existence of the Signal or ProtonMail accounts during his February 2020  
 3       deposition, despite being asked targeted questions on this exact topic. If the switch to these  
 4       accounts was part of an innocuous effort to avoid hacking, Noland could have easily said  
 5       so. His failure to do so raises the inference that the motivation for switching to the accounts  
 6       was more nefarious. *Herzig v. Ark. Found. for Med. Care, Inc.*, 2019 WL 2870106, \*4-5  
 7       (W.D. Ark. 2019) (concluding, where the plaintiffs “install[ed] and [began] using the  
 8       Signal application on their mobile devices” after the dispute arose, and used the Signal  
 9       application to engage in “numerous responsive communications with one another and with  
 10      other AFMC employees,” yet provided an “initial misleading response . . . that [they] had  
 11      no responsive communications” and “did not disclose that they had switched to [Signal]  
 12      until discovery was nearly complete,” that the plaintiffs had engaged in “intentional, bad-  
 13      faith spoliation of evidence” that constituted “an abuse of the judicial process” and  
 14      “warrants a sanction”).

15          The Court also rejects the Individual Defendants’ proffered justification for  
 16      Noland’s failure to disclose the Signal and ProtonMail accounts during his deposition (*i.e.*  
 17      he was confused and/or got cut off by the FTC’s counsel). The deposition transcript  
 18      contains no evidence of confusion or an interruption, Noland also failed to disclose the  
 19      accounts in response to a later question about encrypted communications, and Noland made  
 20      no effort to correct the transcript after the deposition was complete.

21          The content of the ProtonMail email from May 2020, which the FTC lucked into  
 22      discovering despite Noland’s efforts to destroy it, serves as further circumstantial proof  
 23      that the Individual Defendants’ evidence-destruction efforts were not innocuous. 1  
 24      Gensler, *supra*, Rule 37 at 1202 (“[A] court can find intent to deprive based on  
 25      circumstantial evidence.”). As discussed elsewhere in this order, the May 2020 email can  
 26      be construed as an attempt to shape the testimony of third-party witnesses on the key  
 27      disputed issues in this case. If the evidence being destroyed was potentially harmful to the  
 28      Individual Defendants’ case, it is reasonable to infer that their motivations for destroying

1 it were not innocuous.

2 Finally, the coordinated deletion of the Signal app from the Individual Defendants’  
 3 phones in August 2020, just as the phones were about to be turned over for imaging, is the  
 4 *pièce de résistance*. Notably, the Individual Defendants took this step without the  
 5 knowledge or approval of their counsel. This was an outrageous maneuver that raises a  
 6 strong inference of bad faith. *Cf. Ala. Aircraft Indus., Inc. v. Boeing Co.*, 319 F.R.D. 730,  
 7 746 (N.D. Ala. 2017) (“No credible explanation has been given as to why they departed  
 8 from the . . . protocols and intentionally deleted Blake’s information. . . . This type of  
 9 unexplained, blatantly irresponsible behavior leads the court to conclude that Boeing acted  
 10 with the intent to deprive . . .”).

11 This inference is not undermined, in any way, by the Individual Defendants’  
 12 proffered justification for their coordinated deletion effort (*i.e.*, they wanted to prevent the  
 13 FTC from learning the identify of their donors). As an initial matter, this explanation  
 14 makes no sense. If, as Noland testified, the Signal app was set on “auto-delete,” then the  
 15 only information the FTC could have extracted from the Signal apps on the Individual  
 16 Defendants’ phones was their contact lists and call logs—the content of any messages  
 17 would have already been deleted. But seeing a contact list and/or call log would not, on its  
 18 own, tell the FTC anything about which of the Individual Defendants’ contacts were  
 19 donating to their legal defense. Further, the Individual Defendants have asserted ignorance  
 20 as to these persons’ identities. If the Individual Defendants are unaware of this  
 21 information, how could the FTC have gleaned it from a mere examination of their call logs  
 22 and contact lists? More important, putting aside these logical contradictions, the Individual  
 23 Defendants “donor protection” defense fails for the more fundamental reason that they  
 24 were not entitled to take it upon themselves to delete the entire Signal app (which contained  
 25 at least some discoverable, relevant information) simply because they didn’t want the FTC  
 26 to have access to other non-privileged information that might be found in the app.

#### 27 **G. Adverse Inference**

28 The FTC seeks an inference that the spoliated evidence is presumed to be

1 unfavorable to the Individual Defendants. (Doc. 259 at 19-20.) The Individual Defendants  
 2 object to this adverse inference as “yet to be articulated.” (Doc. 276 at 4.) They also assert  
 3 that the FTC’s motion goes to witness credibility more than the loss of potentially relevant  
 4 evidence, so the FTC’s interests can be vindicated through cross-examination rather than  
 5 an adverse inference. (*Id.* at 3-4.) Finally, they emphasize that the prejudice to the FTC is  
 6 minimal because “this case concerns claims of false and misleading marketing and a  
 7 fraudulent compensation plan” and “the overwhelming majority of evidence in this case is  
 8 public knowledge or in the FTC’s possession.” (*Id.* at 4.)

9       It is true that “the severe measures authorized by [Rule 37(e)(2)] should not be used  
 10 when the information lost was relatively unimportant or lesser measures such as those  
 11 specified in subdivision (e)(1) would be sufficient to redress the loss.” Fed. R. Civ. P.  
 12 37(e) advisory committee’s note to 2015 amendment. Nevertheless, the Court concludes  
 13 that the requested adverse-inference sanction is appropriate. As explained above, it is  
 14 likely that the deleted Signal and ProtonMail communications addressed matters relevant  
 15 to this litigation. Further, the Individual Defendants’ conduct violated not only Rule 37(e),  
 16 but also the MIDP (Doc. 14 at 8); the TRO (Doc. 38 at 21), and the preliminary injunction  
 17 (Doc. 109 at 17). These violations raise the possibility of Rule 37(b)(2) sanctions,  
 18 including the drawing of an adverse inference. *See generally Nyerges v. Hillstone Rest.*  
 19 *Grp. Inc.*, 2021 WL 3299625, \*8-17 (D. Ariz. 2021).

20       To the extent the Individual Defendants’ position is that the relevant evidence they  
 21 destroyed in violation of the Court’s orders was insufficiently prejudicial to warrant an  
 22 adverse-inference sanction, this argument lacks merit. The information lost does not  
 23 appear to have been “relatively unimportant” and lesser remedies would be insufficient  
 24 under the circumstances. Indeed, courts have suggested that even stronger sanctions than  
 25 those sought here by the FTC may be permissible to address analogous misconduct. *See,*  
 26 *e.g., WeRide Corp. v. Kun Huang*, 2020 WL 1967209, \*9 (N.D. Cal. 2020) (“The amount  
 27 of spoliation that AllRide concedes is staggering. AllRide admits that it kept its company-  
 28 wide policy of deleting from its server all emails older than 90 days until months after the

1 preliminary injunction issued . . . and that its employees began communicating with  
 2 DingTalk’s ephemeral messaging feature after the preliminary injunction issued. Based on  
 3 these undisputed facts, the Court finds it appropriate to issue terminating sanctions.”);  
 4 *Paisley Park Enterprises*, 330 F.R.D. at 233-34 (“Failure to [turn off the auto-delete  
 5 function] . . . alone is sufficient to show that Defendants acted unreasonably. But that is  
 6 not all the RMA Defendants did and did not do. Most troubling of all, they wiped and  
 7 destroyed their phones after Deliverance and RMA had been sued, and, in the second  
 8 instance for Wilson, after the Court ordered the parties to preserve all relevant electronic  
 9 information, after the parties had entered into an agreement regarding the preservation and  
 10 production of ESI, and after Plaintiffs had sent Defendants a letter alerting them to the fact  
 11 they needed to produce their text messages. As Plaintiffs note, had Staley and Wilson not  
 12 destroyed their phones, it is possible that Plaintiffs might have been able to recover the  
 13 missing text messages by use of the ‘cloud’ function or through consultation with a  
 14 software expert. But the content will never be known because of Staley and Wilson’s  
 15 intentional acts. . . . This is even more egregious because litigation had already  
 16 commenced.”). Accordingly, a general adverse inference is proper. *Cf. Moody v. CSX*  
 17 *Transportation, Inc.*, 271 F. Supp. 3d 410, 432 (W.D.N.Y. 2017) (imposing adverse  
 18 inference sanction when evidence was spoliated with intent to deprive); *Ala. Aircraft*, 319  
 19 F.R.D. at 746-47 (same).

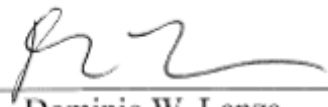
20 Finally, the Individual Defendants suggest that this matter “can better be addressed  
 21 through an evidentiary hearing.” (Doc. 276 at 1.) However, the Individual Defendants  
 22 make no effort to identify the evidence they would attempt to submit during such a hearing  
 23 or explain how it would differ from the voluminous evidence already submitted by the  
 24 parties in relation to the FTC’s motion. No evidentiary hearing is required in these  
 25 circumstances. *Cf. Paladin Associates, Inc. v. Montana Power Co.*, 328 F.3d 1145, 1164-  
 26 65 (9th Cir. 2003) (“Paladin is correct that Rule 37(c)(1) permits a court to impose  
 27 sanctions only ‘after affording an opportunity to be heard.’ However, conforming to the  
 28 rule does not require an evidentiary hearing in every case. . . . Here, Paladin received notice

1 of the possibility of sanctions when MPC filed its motions for costs. It was afforded the  
2 opportunity to respond, and did indeed do so by filing a responsive brief. Given that the  
3 issues were such that an evidentiary hearing would not have aided its decision making  
4 process, the district court did not abuse its discretion in proceeding without an evidentiary  
5 hearing after briefing.”).

6 Accordingly,

7 **IT IS ORDERED THAT** the FTC’s motion for sanctions (Doc. 259) is **granted**.

8 Dated this 30th day of August, 2021.

9  
10  
11   
12 \_\_\_\_\_  
13 Dominic W. Lanza  
14 United States District Judge  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28